Testimony of Glenn S. Podonsky
Director, Office of Security and Safety Performance Assurance
U.S. Department of Energy
Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives

March 18, 2005

Mr. Chairman and members of the subcommittee, thank you for inviting me to testify today regarding the status of security programs in the Department of Energy. The story of security in DOE over the past several years is one significantly affected by change – changes in the global security situation and in the recognized threat we face; changes in the missions and configurations of our weapons complex; and changes in how we approach and practice our security responsibilities. Today I will discuss the progress we have made, amidst those changing conditions, on our efforts to enhance our security posture. I will also discuss those areas in which our efforts have fallen short and in which additional work is needed, and discuss the major security challenges we face over the next few years.

Let me start by reaffirming what I hope the members of the subcommittee fully recognize: the Department understands that we have custody of some of the nation's most vital national security assets, in the form of both information and materials. We know that the protection of these assets is vital to our national security, and we are committed to protecting them. There is no item more important than security on the agenda of the Department's senior management. During the past four years, former Secretary Abraham and former Deputy Secretary McSlarrow championed the cause of security and actively guided our efforts to improve our protection posture. Secretary Bodman has continued that legacy by strongly affirming his commitment to protecting the Department's vital national security assets, facilities, and employees. While we remain convinced that we have in the past, and continue to adequately protect our vital national security assets, we have acknowledged all along that our efforts have not been flawless. We must continually adapt our security programs to a changing world and to an evolving threat environment, and we can and must find ways to further strengthen our security posture. It is with those convictions that we have been aggressively pursuing security improvements during the past four years.

Security Enhancements Since 9/11

The September 11th terrorist attacks made it painfully clear that our long held ideas of postulated threats had become all too real. To ensure that we were adequately protecting our assets against this elevated threat, we knew we needed to take immediate action. Let me summarize some of the things we have done since 9/11 to strengthen the Department's security posture and to contribute to the Nation's security efforts.

On September 11th, we imposed an elevated Security Condition, or SECON, and instituted a number of other actions to increase physical security measures at our facilities, and particularly

around our most sensitive targets. These actions, which varied from site to site depending upon local needs and characteristics, included: increasing the number of protective force posts and patrols; closing key streets and parking areas; and, erecting additional barriers to increase stand-off distances for potential vehicle bombs. Because these enhanced security measures had to be implemented immediately, in many cases our line managers were forced to turn to manpower-intensive solutions involving increased protective force activity. We have been at a heightened state of alert at varying SECON levels, since 9/11.

Our protective forces could not bear this level of burden indefinitely so to relieve that additional burden and seek cost effective and efficient ways to maintain enhanced security, we turned to technology solutions. We selected the very best security technologies available to deploy at our sites, ranging from explosives detection to chemical defense and cyber security. At the same time, we evaluated the human factor associated with highest risk environments. Resulting changes in the Departmental Human Reliability Program have improved the measures by which we assess the physical and mental suitability of individuals who occupy our most critical positions.

We reassessed the Design Basis Threat – the planning basis for our protection requirements – in an effort to ensure that our increased security measures were responsive to our new understanding of the threat. A new Design Basis Threat policy was issued in May 2003. Each site developed implementation plans and began efforts to meet the requirements of the new policy. As a consequence of our efforts to upgrade security since 9/11, our security spending increased from $883M in 2001 to $1.44B in our 2006 request.

The series of Secretarial Security Initiatives announced in May of last year represents the most ambitious and comprehensive of our current security enhancement efforts. The initiatives are broad and far ranging, and impact most major elements of the Department's protection programs, including those of the National Nuclear Security Administration. The initiatives can be grouped into four broad program areas: information security; new security technology solutions; consolidation of materials; and strengthening security human capital expertise. Together, they directly or indirectly impact every aspect of our protection programs. These initiatives are so central to our current effort that is it worthwhile to briefly describe each one and its current implementation status.

One set of initiatives involves **information security**. Much of the information we possess today, including classified information, is created on computers and stored on computer media. Unfortunately, the fast pace of technological development of computer hardware and software seems to be equaled by the pace of development of methods for adversaries to exploit that hardware and software. If we are to continue to operate effectively, we have to actively protect the confidentiality, integrity, and availability of all of the information on our automated systems, and we have to be able to do that even while we are under cyber attack. Consequently, we have to be on the cutting edge of cyber security and must employ tools, systems, procedures, and configurations. Recognizing the urgency of this imperative and the potential consequences of falling behind in this area, we resolved to do more to ensure that our protection systems keep abreast of emerging threats. The three cyber security initiatives are aimed at: increasing testing used to identify (and eliminate) our cyber vulnerabilities before an adversary does; enhancing

protection and training measures within our information security systems; and reducing the exposure of classified information stored on computer media. While these initiatives include some longer-term developmental activities, most can be implemented in the near term. The cumulative effects of these initiatives will significantly enhance our cyber protection abilities. A synopsis of each of these three initiatives and our current progress in achieving full implementation follows.

- Expand Cyber Security Performance Testing. This initiative expands our independent oversight organization's cyber security performance testing program for both classified and unclassified information systems by: expanding the scope and increasing the frequency of unannounced penetration testing; conducting continuous scanning of unclassified computer systems to reduce the exposure to Internet threats; and expanding testing of classified computer networks to ensure appropriate need-to-know protection boundaries are in place and are effective.

  The institutional structures necessary to implement this initiative have been put in place, and expanded testing has already begun. The necessary additional personnel, computer systems, and testing tools have been procured and operating procedures and testing protocols have been validated. Expanded unannounced penetration testing and enhanced testing of classified systems has commenced. We are preparing to begin continuous network scanning and penetration testing to reduce Internet exposure, starting with Headquarters and subsequently phasing in additional sites.

- Cyber Security Enhancements. This initiative consists of integrated steps intended to protect the confidentiality, integrity, and availability of our information systems by quickly disseminating cyber threat information, expanding intrusion detection systems that rapidly identify cyber attacks, reducing the exposure of our information systems to Internet threats, and improving workforce cyber security training.

  DOE's Chief Information Officer is leading the efforts associated with this initiative. To date, we have: increased inter- and intra-agency sharing of cyber threat and vulnerability data; incorporated intrusion detection and prevention into our cyber security enterprise architecture; completed independent reviews of Headquarters implementation of the Department's Cyber Security Management Program; upgraded cyber security training programs; and developed a methodology to identify inappropriate information on publicly accessible websites. This methodology was applied to an initial website cyber security analysis.

- Diskless Desktop Computing. The use of Classified Removable Electronic Media (CREM) to store information has been a persistent security challenge, primarily due to the ubiquity of the media. This initiative seeks to eliminate or greatly reduce this challenge by moving, within a five-year period, to diskless workstations for classified computing. The National Nuclear Security Administration has been tasked to identify and implement appropriate diskless technologies. Successful technologies will then be implemented Department-wide.

A "tiger team" completed a review of potential technical and management solutions to this issue. The team identified requirements for providing high-speed desktop workstations and proposed a set of standard diskless workstation solutions, cost estimates, and related recommendations. On January 31, the former Deputy Secretary directed the formation of a Project Management Office within NNSA to manage implementation of this initiative.

Another set of initiatives involves the development and deployment of new **security technologies**. Two of the security initiatives are aimed specifically at enhancing our protection programs through increased use of security technology solutions. One is focused on addressing an area that has been associated with several security incidents – specifically, replacing lock and key systems in security areas with modern, keyless entry control systems. Although fairly narrow in scope, this initiative represents a massive undertaking, given the number of locks and keys currently in use at our security areas throughout the complex. The other security technology initiative is a much broader effort aimed at identifying, evaluating, or developing a broad range of useful technologies and facilitating deployment at DOE sites. We are particularly interested in identifying technologies that can help our protective forces better counter the ever-changing threats to our national security assets. Properly applied, such technologies can act as force multipliers to assist our protective forces by reducing the burden of routine activities, reducing the risk to them in case of an attack, and, through enhanced recognition, provide additional response time to meet and defeat an attack.

- Keyless Access Control Technology. NNSA is researching and identifying suitable technology that will enable the Department to transition, over a five-year period, to a keyless security environment where no single item that provides access to protected assets, can be lost or stolen.

  We are making progress in this area. My office has developed a current technology matrix that provides specific descriptions of keyless systems, their costs, and locations where they are currently in use. The NNSA formed a multi-organizational Technology Review Team to analyze these alternatives. Additionally, the efforts of the Integrated Project Team which is addressing HSPD-12 – the Policy for a Common Identification Standard for Federal Employees and Contractors, which requires "smart cards" for physical and logical access to Federal sites, buildings, and systems, will complement these efforts.

- Blue Sky Commission. This initiative involves the identification of off-the-shelf security technologies available for rapid deployment and the establishment by NNSA of a Blue Sky Commission to evaluate promising emerging technologies that the Department can invest in or develop to enhance our future protection systems.

  While we are taking action to identify and apply existing technologies to enhance our protection systems, we have not yet taken the formal steps necessary to coordinate investment in emerging security technologies. The Technology Development Program, within my organization's Office of Security, has disseminated information about current off-the-shelf items suitable for integration into security systems. Last July we established the Center of Excellence for Technology Deployment at Pacific Northwest National Laboratory (PNNL) in Richland, Washington. The Center's mission is to find technologies with security

applications that are deployable today; to assist in implementing pilot programs at DOE sites to test those technologies; and to assist in the further deployment at other DOE sites of those technologies that prove to be effective and useful. Let me emphasize that this Center's job is not to develop new technologies, but rather to seek out new technologies that are available today and to expedite their evaluation and, when appropriate, their speedy integration into security systems at DOE sites. In an effort to assist sites in choosing appropriate technologies to implement the current Design Basis Threat, we are in the final stages of a series of Site Assistance Visits to our facilities possessing Category I quantities of special nuclear materials. During these visits, our multi-organizational, multi-discipline teams work with site security personnel to analyze the existing and future site-specific protection systems and identify security technologies that could be employed to increase the effectiveness and efficiency of those systems. This effort, which I will come back to in my discussion of the Design Basis Threat, has been beneficial to the sites. Our progress in enhancing our efforts to identify and invest in the development of emerging technologies has been somewhat slower. Although we anticipated that NNSA would formally establish the Blue Sky Commission last October, that action has yet to occur.

Before I leave this topic, let me mention some of the progress we have made in technology deployment. Several technologies have recently been deployed at sites throughout the complex to significantly improve their ability to mitigate our Design Basis Threat policy. For example, newly developed armored vehicles with advanced fighting capabilities are being deployed at two sites. These vehicles will allow protective forces to be forward-deployed and engage adversaries earlier, while relying on improved armor to increase their survivability and externally mounted weapons and optics to neutralize adversaries. Chemical agent detectors are also being deployed at six locations. These detectors are unique in that they are able to operate 24 hours a day for extended periods (years), require minimal maintenance, and provide sufficient time for response forces to don protective gear and engage the adversary. Unmanned Aerial Vehicles UAVs are also being deployed to help conduct surveillance of vast areas outside of a large remote site. The UAVs will be equipped with sensors that will detect the adversary earlier, and deny them the luxury of being able to pre-stage attackers and equipment and initiate an attack at a time that is advantageous to them. The UAVs will also be used to improve combat situational awareness should the site come under attack. One of the threats seen almost every day in the news is the large vehicle bomb, lending credibility to our need to defeat it. A new type of affordable ($300/ft) vehicle barrier has been deployed at one site, and is being installed at a second. What makes this barrier unique is its ease of installation, and its ability to stop very large vehicles moving at highway speeds. We are also in the final stages of deploying remotely operated weapons at one of our facilities, before expanding the deployment to other sites. These weapons are a formidable barrier for the adversary, particularly when deployed with visual obscurants. Not only do we expect them to improve our ability to neutralize adversaries, but they will also improve the survivability of protective forces in fire fights and situations where an adversary might use lethal chemicals. Our future plans call for assisted targeting to be integrated into these weapons, and we are hopeful that this will eventually lead to manpower savings by proving that an operator can control more than one weapon. We believe that the expanded application of security technologies, such as those just described, will be critical to the successful mitigation of the evolving and increasingly capable threats we will face in the future.

A third set of initiatives addresses our need to **consolidate our inventories of special nuclear materials.** Our successes in consolidating significant quantities of special nuclear materials have typically been limited to facility closure programs, such as at the Rocky Flats Environmental Technology Site. While we still need special nuclear materials at some sites to accomplish ongoing national security missions, both the amount of materials needed and the number of locations where they are needed have substantially decreased since the days of the Cold War when our production facilities were building our nuclear deterrent. Protecting these materials is among our most difficult security challenges, but it is also one of our most important missions, since the consequences of their loss are unacceptable. We can greatly reduce the difficulty, risk, and costs associated with protecting this material if we can consolidate that which we cannot safely and properly eliminate. This has become an increasingly important consideration with the increased difficulty and costs associated with defending against the elevated threats described in the current Design Basis Threat. Since reduction and consolidation of special nuclear materials has perhaps the greatest potential impact on our future protection requirements and programs, we have identified seven separate initiatives related to this subject. These initiatives range in scope from developing plans for terminating the use of a reactor to altering the configuration of the Department's weapons complex. This group of initiatives addresses the essential challenges we face in our efforts to reduce and consolidate our special nuclear materials inventories and to accurately assess the threats to these materials,

- Sandia Pulsed Reactor. This initiative involves completion of the Sandia Pulsed Reactor's mission and removal of the special nuclear material (reactor core) from Sandia National Laboratories-New Mexico.

  To enhance the reactor core's physical protection, Sandia has disassembled it and placed it in special protected storage until needed to support essential testing. The reactor will be re-assembled and used for a period of approximately one year to support testing and to qualify theoretical models and simulation methods that will eliminate future needs for the pulsed reactor. Upon successful completion of the test series, the reactor material will be returned to a secure storage condition that greatly reduces the security risks and cost. The testing and modeling work is currently planned to support the cool down and completion of reactor defueling by March 2007.

- Highly Enriched Uranium Materials Facility (HEUMF). This initiative is to expedite the construction of the HEUMF project, which will provide a new state-of-the-art storage facility for highly enriched uranium now stored at various locations at the Y-12 National Security Complex. Its design will incorporate a robust denial strategy that includes passive design features to address the DOE Design Basis Threat Policy. Goals of completing facility construction and readiness activities by April 2008 and relocating existing material from current locations into the new facility by September 2009 will greatly enhance the security of highly enriched uranium within the United States and decrease long term operating and material safeguarding costs at Y-12.

  The primary facility construction contract was awarded on schedule on August 27, 2004. Construction is currently 9% complete, including site preparation. While construction is approximately two months behind schedule due to above normal rainfall and unanticipated

soil conditions, it is expected that the original schedule will be met. Associated activities, such as storage container assessment and characterization and material movement and reduction of material in current storage areas are underway.

- Resolve Materials Criteria for Acceptance at Long-Term Storage Sites. This initiative addresses the need to resolve situations where nuclear materials are being stored at sites only because they do not meet the acceptance criteria at longer-term storage sites. Increases in the Department's Design Basis Threat necessitate creative approaches to maintain strong security for the Department's special nuclear material assets in a cost-effective manner.

  A Nuclear Material Consolidation Task Team studied the issue of materials consolidation with a focus on reducing the number of nuclear facilities that need high-level protection and reducing the number of potential terrorist targets. A draft report was issued in December 2004. The report identifies and prioritizes candidate materials for consolidation using a set of defined criteria which address security impact, schedule, cost, and programmatic use. The report also provides recommendations for implementation in both the near, mid, and long term. To formally institutionalize this important effort and to cut across programmatic lines, a multi-program senior-level steering group, under the direction of the Secretary's Senior Policy Advisor for National Security Matters, will provide guidance and recommendations to the Secretary on nuclear material consolidation issues.

- Weapons Complex Review. This initiative involves reviewing the requirements for the weapons complex for the next 20 years in light of the size of the stockpile, the new Design Basis Threat, and the opportunities for consolidation, with the goal in mind of reducing the footprint of the complex to the minimum needed to support long-term national security missions.

  The Secretary of Energy Advisory Board (SEAB) chartered a Task Force which consists of five members who were briefed by members of the Department of Defense, National Security Council and NNSA Program Offices in February. The Task Force has visited most of the weapons complex facilities and will complete their tour by mid-April. Once the study is complete and consolidation opportunities are identified, we anticipate that political (e.g., involving moving material between states) and programmatic (e.g., construction) barriers will remain to be confronted.

- Down-blend Large Quantities of Highly Enriched Uranium (HEU) to make it unattractive as a terrorist target. The goal of this initiative is to determine whether, via the early disposition and down-blending of up to 100 metric tons of HEU currently stored at the Y-12 National Security Complex, we could strengthen the security of existing HEU operations and storage at that facility.

  Review results recommended a course of action to increase the security of remaining HEU and promote the President's nonproliferation objectives. The review recommended that a substantial quantity of HEU be removed from any future use in nuclear warheads. This is in addition to the 174 metric tons of HEU declared in 1994 to be in excess of national security

needs. The NNSA Administrator endorsed the recommendations of the study and directed coordination with the Departments of Defense and State.

- Design Basis Threat (DBT) Reexamination. This initiative reexamined the May 2003 DBT and the supporting intelligence data to ensure currency in relationship to the changing threat.

  Actions on this initiative are complete. The DBT was reexamined, changes were recommended, and on October 18, 2004, the Deputy Secretary approved DOE Order 470.3, "Design Basis Threat (DBT) Policy" for implementation. In conjunction with the DBT revision, we revised the Adversary Capabilities List to reflect the most current intelligence information regarding the observed and postulated capabilities (e.g., weapons, equipment, tactics, etc.) of the adversary. Although this initiative is complete, follow-on activities through April 2005 are focused on conducting the Site Assistance Visits mentioned previously to provide sites with technology and protective force tactical options to address the requirements of the October 2004 DBT Policy. I will discuss the Design Basis Threat and its impact on protection strategies and systems in more detail later in this testimony.

- Removal of Category I/II special nuclear materials (SNM) from TA-18. The object of this initiative is to relocate programmatic SNM from Los Alamos National Laboratory's (LANL) Technical Area -18 to the Device Assembly Facility (DAF) at the Nevada Test Site.

  Implementation of this initiative is in progress. On March 31, 2004, NNSA directed the initial shipment of LANL TA-18 programmatic SNM to the DAF ahead of the previously scheduled date of March 2006. Three shipments of programmatic materials were completed as of December 2004. Approximately seven shipments are planned for FY2005. NNSA currently projects that approximately 50% of the TA-18 programmatic SNM will be moved to the DAF by March 2006 and 90% by the end of fiscal year 2007. Programmatic SNM needed by NNSA to maintain mission continuity, especially to support training for Emergency Response, will remain at LANL in other storage locations.

The final set of initiatives concern our **security human capital**. Of all the components of our protection systems, the human component is the most critical, and the performance of our people will largely determine the success or failure of our protection efforts. When we speak of security personnel in this context we refer to two groups of people: the people who develop, implement, maintain, and oversee our security programs; and the protective force personnel who are on the ground 24/7 protecting our assets. The robustness of our protection programs depend largely on the abilities and performance of these two groups of people. Three of our security initiatives deal with strengthening our security human capital. They include efforts to implement the recommendations of the Chiles Commission (regarding management of security expertise in the NNSA) within the NNSA and possibly throughout the entire Department. In addition, the initiatives also address options for protective force configuration and management, with special emphasis on determining the best approach for creating an elite force dedicated to protecting our most critical sites.

- Implement Chiles Report recommendations. The Chiles Report focused on the NNSA nuclear weapons complex and recommended several actions to resolve impending human capital shortfalls

in safeguards and security and related disciplines. Specific recommendations involved: developing and executing a comprehensive human capital management program; improving the training, qualifications, and stature of the workforce; reengaging in national markets to hire security professionals; instituting a long-term practice of security staff rotation; identifying options for accelerating the security clearance process; improving security information flow; revising the NNSA Safeguards and Security Strategic Plan; identifying specific budget support and tracking recommendation progress.

NNSA is actively pursing implementation of this initiative. For example, to address human capital management, workforce analysis methodologies and protocols were piloted at the Pantex Site Office. Five professional development data assessments were completed at the Pantex Site Office, Y-12 Site Office, Sandia Site Office, Nevada Site Office and the NNSA Service Center. This same assessment is also planned for the Los Alamos Site Office. NNSA is partnering with the DOE National Training Center to provide centralized training for safeguards and security professionals to meet qualification standards established for each safeguards and security functional area. Additionally, NNSA has developed a web portal to improve security information flow, implemented a process for rotating security management positions between headquarters and the field, and began recruiting for an Intern Program.

- Examine the Applicability of the Chiles Report recommendations to the Department. This initiative calls for an examination of the Chiles Report recommendations – which were addressed to the NNSA – to determine their applicability and appropriateness to enhance security human capital and training programs throughout the Department.

  The human resource challenges facing the Department were identified previously and analyzed in the context of the President's Human Capital Management Plan. Efforts have been underway at our National Training Center to promote skills development in identified critical areas through on-going Professional Development Program activities. The first four recommendations of the Chiles Report are being implemented through activities at the National Training Center and through the Human Capital Management Plans developed by my organization, the Office of Security and Safety Performance Assurance, and by the Under Secretary for Energy, Science, and Environment. Concerns regarding the lengthy clearance process are being addressed through ongoing implementation of the approved action plan entitled "Options for Accelerating the Security Clearance Process in the Department of Energy" signed by the former Deputy Secretary on January 7, 2005. My organization addressed security communications concerns following the completion of a Communications Study Report last July, and a DOE 25-Year Strategic Security Plan is pending review and approval by the Under Secretaries.

- Review Options for the Protective Force. This initiative directs the examination of existing protective force organizational structures (including existing contract mechanisms) to determine changes needed to develop an elite protective force. The ultimate goal is to transform the protective forces that guard our most critical national security assets into elite units, trained and equipped for advanced tactical operations, and comparable in capability to the nation's elite military units.

  Actions on this initiative are complete. This review was completed and a final report containing recommendations was provided to Senior DOE Management. A joint memorandum from SSA and

NNSA was submitted to the former Deputy Secretary in January of this year, recommending that those actions that could be initiated within the current force structure be approved. The Deputy Secretary directed immediate implementation, which is now ongoing. Follow-on activities continue relative to implementation of the identified options resulting from the review.

Mr. Chairman and members of the Subcommittee, we have made significant progress in our efforts over the past several years to improve our protection systems. The security initiatives I have just outlined, and the ongoing and planned actions, represent a sizeable effort and significant commitment of resources by the Department aimed at addressing past security concerns and materially enhancing our present and future protection postures. Our work to implement many of these initiatives continues, and in some cases will continue for several more years. I believe that the progress we have made to date in implementing these far-reaching initiatives, while significant, will pale in comparison to the benefits that will accrue to our protection programs when the initiatives are fully realized.

Ongoing Security Challenges

The job of adequately protecting the Department's national security assets is an immense undertaking. While we are aggressively pursuing actions to address known deficiencies and improve the robustness of our protection systems, we recognize that we have a lot more to do.

As evidenced by our need for the security initiatives and other previously described enhancement activities, we continue to experience problems associated with both management systems and program implementation. Our independent oversight organization has indicated for years that many local line management feedback and improvement mechanisms, such as Federal security survey programs and contractor self-assessment programs, were not sufficiently comprehensive or adequately performance based to effectively detect and correct all existing protection program deficiencies. This is verified by problems we found at sites such as Hanford, Oak Ridge National Laboratory, Sandia National Laboratories-New Mexico, Y-12, and the Nevada Test Site. These problems, which included such things as poor protective force tactical performance, deficient nuclear material control and accountability programs, and inadequate classified document controls, should have been identified and corrected by local line management feedback mechanisms before we found them during our inspections. I must acknowledge, however, that once we identified problems at these sites the local line managers were responsive in taking action to correct them. Our Independent Oversight organization similarly reported slow progress in implementing Integrated Safeguards and Security Management processes, and we have continued to experience other protection system problems that are directly related to inadequate line management oversight, attention, and accountability.

For example, in the past few years we experienced several highly publicized incidents involving the loss of keys or key cards affording access to buildings or rooms within security areas at a few of our facilities. Although there is no indication that these losses resulted in compromise of classified information or other security assets, they are disturbing nonetheless. A review of lock and key programs revealed that management attention to these programs was largely absent. As a result, there were too many spare keys, no strict accountability for all keys, and inadequate

accountability/security training for lock and key program personnel and key custodians. These incidents were among the motivations behind our initiative to transition to a keyless security environment at some facilities.

Another recent problem involved control and accountability of Classified Removable Electronic Media (CREM) – computer floppy disks and such. As I am sure the members of the subcommittee are aware, last year the Department discovered that we had some deficiencies in our procedures and practices for handling and protecting the classified information contained on CREM. An incident at Los Alamos National Laboratory – which subsequent DOE and FBI investigations determined did not involve the loss of CREM – raised questions about accountability systems and control procedures for handling CREM. Even though our Independent Oversight organization had been reporting conditions that could lead to such an incident, local line managers in many cases failed to give sufficient attention to this matter. While we acknowledged the obvious fact that incidents such as this can occur, we do not concede that they must inevitably occur. We simply will not tolerate continued incidents of this nature. In order to ensure that conditions that would allow a similar incident to occur do not exist anywhere in the Department, the Department's senior management took a series of aggressive, even unprecedented actions. For the first time in the Department's history they ordered a complete cessation of all classified operations involving accountable CREM. Facilities were not allowed to resume those operations until they fully complied with a set of restart protocols, whose key aspects included:

- Ensuring and certifying that all employees who handle accountable CREM receive training in proper handling procedures and have reviewed information regarding the incidents at Los Alamos.

- Conducting a 100% physical inventory of all accountable CREM on hand and reconciling that physical inventory with baseline inventory records.

- Implementing strict requirements and procedures for the storage of CREM (pertaining to approved repositories, keeping repositories locked except when removing or replacing CREM, use of security seals on repositories, etc).

- Limiting access to each repository containing accountable CREM to one Custodian and one Alternate Custodian, and establishing and performance testing formal checkout processes for authorized users to obtain accountable CREM from a Custodian or Alternate.

- Conducting weekly physical inventories of all accountable CREM, and reconciling the inventories with accountability records.

- Establishing procedures which ensure that accountable CREM is destroyed only by approved DOE destruction procedures and which assure that accountable CREM is reproduced only if authorized by the specifically appointed Federal authority.

- Ensuring that a local CREM validation team independently verifies, using performance testing, the implementation and effectiveness of all restart protocol requirements.

The former Deputy Secretary, designated by the Secretary, was the only person who could authorize a facility to resume operations with accountable CREM, once they satisfied the restart protocols. All of our facilities have satisfied the stringent requirements and have resumed operations with accountable CREM.

Following this process, my Office of Independent Oversight and Performance Assurance sent teams of experts to our major facilities to perform additional independent validations, to make sure that that the restart protocol requirements were fully and effectively implemented. Various problems were observed during this validation step. For example, the Nevada Site Office/Nevada Test Site needs to establish a centralized accountability system to improve efficiency; Los Alamos required a lengthy period to achieve restart of classified operations and the quality of their revised procedures still requires validation.

As evidenced by these unprecedented measures, we are serious about protecting our classified information and about ensuring that additional incidents involving the protection of CREM do not occur at any of our facilities. While our intended move to a diskless desktop classified computing environment will largely eliminate the potential for such incidents, the use of CREM will be common for at least the next several years, and we will maintain strict enforcement and oversight of our current requirements for handling CREM.

As a final example of our experiences with insufficient line management attention to security programs, let me address the results of our Review of NNSA's Federal Line Management Oversight of Security Operations. Our Office of Independent Oversight and Performance Assurance conducted this review at the direction of the Secretary. Data collection methodologies included reviews of the results of other recent studies that had examined this issue in whole or in part. These included Independent Oversight reports, the Chiles and (draft) Mies Reports, and the reports of internal focus groups studying various security-related Departmental management challenges. The review identified or confirmed a number of issues that reflect significant weaknesses affecting the performance of line management oversight responsibilities. These include:

- NNSA has insufficient personnel resources and expertise assigned, particularly at site offices, to effectively conduct the quantity and quality of oversight activities necessary to reliably determine or assure the effectiveness of site safeguards and security programs. The general aspects of the shortage of security expertise at appropriate locations in NNSA are multi-faceted, involving work force demographics, recruitment efforts, training and education opportunities, career path opportunities, and resistance to geographical relocation. The specific problem at NNSA site offices, where it currently has the greatest impact on security oversight, is manifested in two ways: in the numbers of security professionals available and in the skill mixes represented by currently assigned personnel.

- NNSA site office survey programs are not sufficiently effective in assessing the adequacy or effectiveness of site safeguards and security programs. Surveys are a primary oversight tool available to the site offices. Many survey programs are not effectively or reliably achieving their primary goal, which is to accurately determine the effectiveness of site safeguards and security programs.

- NNSA does not consistently apply or enforce appropriate corrective action program requirements on site contractors. DOE has specific requirements for the corrective action process that is to be applied to all formal findings assessed against safeguards and security programs by Federal oversight activities. NNSA oversight responsibilities are an integral part of that process, but in common practice, this process is often not fully invoked or enforced by the NNSA site offices.

- NNSA has not effectively taken advantage of the opportunity to use award fees and performance incentives to spur intended results in safeguards and security program performance**.** Site offices have generally been ineffective in appropriately emphasizing security through contractor performance incentives and in formulating performance indicators that are successful in achieving the intended results.

These issues have all been identified through internal oversight activities and/or through the efforts of independent teams commissioned by NNSA. DOE, including NNSA, managers have initiated the following significant actions to address these issues and to improve Federal line management oversight of NNSA security operations.

- DOE, including NNSA, is taking steps to address shortages in security manpower resources**.** As part of the security initiatives announced in May 2004, the Secretary of Energy directed NNSA to implement the recommendations contained in the Chiles Report, several of which deal with (security-related) human capital management. NNSA actions associated with this initiative were discussed above.

- NNSA has initiated actions to address the education and training needs of its Federal security workforce, including those specifically applicable to oversight responsibilities**.** NNSA is working closely with SSA's National Training Center to expand the course offerings in the Professional Development Program to encompass identified NNSA needs, including curricula in leadership and management development, incumbent training in safeguards and security technical disciplines, and training and orientation for security interns. In an immediate action to expand the experience level of security professionals, NNSA has implemented a rotation program to afford security professionals in the field the opportunity to work at headquarters and security professionals at headquarters the opportunity to work at field sites. At present, two individuals are participating in this program.

- DOE, including NNSA, is taking positive steps to clarify and strengthen Federal oversight responsibilities at various management levels. Draft DOE Policy 226.1, *DOE Oversight*, and a corresponding DOE Order are currently in the review process. They are intended to clarify and assign oversight responsibilities, including those of headquarters organizations. NNSA is currently implementing a Defense Nuclear Security Performance Assessment Program that integrates Federal line management oversight activities. In furtherance of this objective, NNSA has recently established an Office of Performance Assurance to head this effort.

- NNSA has increased its efforts to reorient day-to-day oversight of contractor security operations**.** Senior managers are involved in an effort to alter the previous philosophy of telling the contractor the ultimate goal (what to do) and allowing the contractor to decide how to reach the goal (how to do

it). While avoiding actions that might stifle contractor initiative, NNSA is encouraging site office personnel to focus more attention on how contractors are performing security operations and to provide more input to contractors regarding preferred methods of operation.

Our review concluded that while these deficiencies in line management, and their underlying conditions, exist and have been adversely affecting NNSA's ability to exercise adequate line management oversight of security operations, the problems are known to NNSA and the Department, including NNSA, has initiated actions to address them. While solutions to these issues are being pursued, some of those solutions – such as increasing the security workforce and implementing necessary training and education programs – will take several years to implement fully, and will require the sustained support of DOE, including NNSA, senior managers.

We also acknowledge that, while protection programs at our sites are generally effective overall, potentially significant lapses in protection program implementation do sometimes occur at our NNSA sites as well as at sites under the purview of the Under Secretary for Energy, Science, and Environment (ESE). For example, at Oak Ridge National Laboratory (an ESE site) portions of the protection system lacked the defense-in-depth that we require, and the site relies on an agreement with a neighboring site for special response team (i.e., offensive combative) capabilities. Our most recent Independent Oversight inspection at the Hanford site (ESE) found that the protective force needed to improve its tactical training, planning, and skills, and that some local human reliability program processes required reexamination. Since that inspection, the Hanford site has implemented corrective actions designed to correct these deficiencies.

Our three most recent Independent Oversight inspections at NNSA sites (Sandia National Laboratories-New Mexico, Y-12, and Nevada Test Site) identified some common implementation problems, including insufficient frequency of large scale force-on-force performance testing/exercises and inadequate weapons and equipment to fully deal with today's threat (e.g., armored vehicles, anti-armor weapons, weapons with high rates of fire). Additionally, the Nevada Test Site exhibited deficiencies in protective force operations and material control and accountability procedures; Sandia exhibited deficiencies in physical security systems and in handling classified matter; and Y-12 exhibited significant deficiencies in most major protection program elements. Since those deficiencies were identified, line managers have been responsive and the sites have been engaged in corrective actions. Our Independent Oversight organization is currently inspecting Sandia-New Mexico to determine its current protection system status and the progress it has made in addressing deficiencies. It will inspect Y-12 in May and June and the Nevada Test Site in July and August of this year.

When implementation problems such as those described do occur, we do not ignore them. We employ a formal corrective action and validation process to ensure that identified problems are fixed, and in cases where a deficiency results in a potential vulnerability, immediate compensatory measures are required. I would also like to point out that as we continue to make Department-wide progress on the security initiatives discussed above and in our system upgrades in response to the requirements of our current Design Basis Threat, we expect that our protection programs will become more robust and the historically troublesome protection elements (e.g., locks and keys, CREM, training, etc.) will be addressed through these efforts (specifically through the application of technologies or other solutions).

The last security challenge I would like to discuss is perhaps our major challenge – implementing the requirements of our new Design Basis Threat. After a prolonged development process, the Department issued a revised DBT in May of 2003. In May of 2004 – in response to internal concerns, Congressional concerns regarding the robustness of the threat portrayed in the DBT relative to that portrayed in the Defense Intelligence Agency's Postulated Threat, and questions raised by the General Accountability Office – the Secretary directed the NNSA Administrator, the Director of the Office of Intelligence, and me to reexamine the May 2003 DBT and its supporting intelligence data to ensure that it was still current in relationship to the changing threat. We formed a task team comprised of individuals with the expertise necessary to assist in conducting the review, and the results of that effort were reported to the Secretary in late August 2004. In October 2004 the former Secretary approved a revised DBT, one which included some significant changes from the previous DBT. Since the DBT is classified, I cannot discuss some of its specific provisions in this open forum, but I will discuss some of its generic attributes and comment on some of the differences between the current and previous versions.

Our DBT policy is intended to provide consistent and appropriate safeguards and security system performance specifications that Departmental elements must meet. It delineates a graded threat scale based on the sensitivity of the asset being protected and the potential consequences of asset loss. Assets are categorized into one of four "Threat Levels" based on the general consequences of their loss or destruction, or the possible impact of their loss or destruction on the health and safety of employees, the public, and the environment. The protection requirements for those assets are graded in a commensurate manner. Performance-based standards must be met to protect Threat Level 1 (most critical), 2, and 3 facilities and assets. Threat Level 4 (non-critical) facilities and assets must meet compliance-based standards**.**

The most significant changes reflected in the current (October 2004) DBT are:

- The policy now exists as a formal DOE Order. Procedures requiring a formal annual review have been issued.

- The policy is more concise, and understandable, and the number of Threat Levels applying to various assets and facilities have been combined and simplified. Threats associated with improvised nuclear devices and radiological, biological, and chemical sabotage have been folded into the Threat Levels.

- The terrorist numbers and attributes associated with the threat levels were increased to reflect current intelligence and geopolitical assessments.

In December 2004 the former Deputy Secretary directed that all DBT implementation plans be revised to ensure that all requirements contained in the October 2004 DBT are met no later than the end of FY 2008. The NNSA Administrator has expressed his full support and intention to develop and execute implementation plans on schedule. However, full implementation of the DBT on schedule is a major task posing many difficulties. For example:

- At some facilities it will require fundamental departures from institutionalized protection strategies, such as shifting from a containment strategy (preventing an adversary from

escaping with target material) to a denial strategy (preventing an adversary from reaching target material).

- The postulated impacts of the DBT mandate that the Department consider aggressive material consolidation efforts, which will likely encounter operational, programmatic, and political opposition.

- The adversary numbers and capabilities postulated in the DBT allow the adversary much greater tactical flexibility, causing significant planning and response difficulties for current security systems.

- The appropriate security technology solutions are still being identified and developed. Consequently, developing accurate budget estimates is difficult at this time.

- Sources of funding and alternatives to current operations that will be necessary to implement the DBT are still being explored.

We are fully cognizant of these difficulties and are prepared to deal with them. We believe that the current initiatives that will contribute most to our DBT implementation efforts are: increasing the use of security technologies, implementing the elite protective force concept at select facilities, and consolidating our special nuclear materials to the greatest practical degree. As mentioned earlier, our Site Assistance Visit effort – now underway and almost complete – is intended to apply our best technological, analytical, and tactical expertise to assist our most critical facilities in identifying security technology applications and innovative protective force strategies that will enable them to effectively and efficiently meet the requirements of the DBT. So far we are encouraged by the progress resulting from these visits. Individual sites will have to follow up that effort with detailed vulnerability analyses to finalize the designs and compute the costs of their proposed protection system upgrades. Ultimately, we will have to devise ways to integrate new security technologies and new protective force weapons and tactics with operational needs and safety concerns.

Conclusion

In closing, we believe the Department of Energy under the leadership of Secretary Bodman is, and will continue to, actively pursue initiatives that will improve the capabilities of our security systems and procedures, and we have forcefully responded when elements of those systems have not performed according to our expectations. We will continue seek innovative, effective, and efficient methods, as well as the resources, to foster the changes in our security programs and practices that are necessary to effectively counter the evolving threat.

Thank you.